

2. A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity means/information ;

said identity means/information will be determined as existing , if the result of said authentication is favourable and as not existing if otherwise .

3. (second time Amended) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being [a] first software used on said processing device for determining third information related to hardware and/or software of said processing device ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing device, basing on at least a part of said third information;

and access to [a] third software will be provided if said authentication result is favourable .

[wherein said third software being distributed through a communication network to said rightful user]

15. A method for protecting software from unauthorised use , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

16. (Second time Amended) A method for protecting software distributed by a system from unauthorised use , comprising the steps of :

- a) obtaining by a processing means of said system, confidential information of rightful user(s) of said software desired to be protected ;
- b) creating by said processing means, [a] first software with said confidential information therein ;
- c) transferring from said system, said first software to a processing device [under control of said rightful user(s)] ;
- d) [thereafter]obtaining by said first software running on said processing device , first information from the user thereof ;
- e) determining by said first software, from said processing device second information related to the hardware or/and software thereof for future reference in step f) below, in response to said first information obtained being consistent with said confidential information therein ;
- f) thereafter, authenticating by [a] second software, the processing device onwhich said second software is being used, basing on at least a part of said second information ;
- h) using, by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;
wherein said confidential information is necessary for enabling electronic transaction(s) for which said rightful user(s) has to be responsible ; and said steps d) to h) is being performed without causing a said tranaction take place .

17. (First time Amended) A method for protecting software [distributed by a system] from unauthorised use, as claimed by claim [16] 12, wherein [“said first information obtained being consistent with said confidential information” being the only condition for performing said determination in said step e)] said software desired to be protected being purchased commercial software.

18. (First time Amended) A method for protecting software from unauthorised use, comprising the steps of :

- a) transferring from a software distribution system, said software desired to be protected to a processing device [under control of a user] ;
- b) transferring from said software distribution system, [a] first and second software which being specific to a user, to said processing device ;
- c) [determining by said first software running on said processing device, say first processing device, if identity information/means which being essentially used by a control means of said processing device for accessing in a remote electronic transaction system an account of said user, is present in said processing device ;]
- [d)] establishing a communication between said first software running on said processing device, and a control means of [said] a remote electronic transaction system ;
- d) [for] verifying said [account is] user having a valid account, by said control means of said remote electronic transaction system to said first software ;
- e) using by said first software, a favourable [results] result of said [determination of presence and] verification as [pre-conditions] a pre-condition for determining from said processing device information related to the hardware or/and software thereof, for future reference in step f) below ;

wherein a cost is being charged from said user by said software distribution system, for [the first time] said steps a) to e) being carried out ; thereafter

- f) authenticating by said second software, the processing device onwhich said second software is being used, say, second processing device, basing on at least a part of said information related to said hardware or/and software ;

- g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing device, with no charge ;

if the result of said [determination of consistence] authentication is not favourable, repeat at least said steps c) to g) with said second processing device, without re-charging from said user said cost .

[wherein said first and second software being specific to said user.]

19. (First time Amended) A method for protecting software [distributed by a system] from unauthorised use, as claimed by claim 18, wherein no charge by said software distribution system for repeating at least said steps c) to g) .

20. (First time Amended) A method for protecting software distributed by a system [through a communication network,] from unauthorised use, comprising the steps of :

- a) creating by said system, [a] first software ;

wherein “the presence of identity information/means which being essentially used by a control means of a processing device for enabling operation(s) for which a rightful user of said software desired to be protected has to be responsible, in said processing device” ; is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ;

- b) transferring from said system, said first software to said processing device ;
- c) determining by said first software running on said processing device meeting said precondition, first information related to the hardware or/and software of said processing device , for future reference in step e) below ;
- d) thereafter, determining by [a] second software, from the processing device onwhich said second software is being used, second information related to the hardware or/and software thereof;
- e) determining by said second software, if said second information is consistent with said first information ;
- f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

repeat at least said steps c) to f) if said result of said determination of consistence is not favourable, without causing any operation(s) for which said rightful user has to be responsible, being performed ;

wherein said first and second software being specific to said rightful user.